3123 93130199

Selection of a secret key at random from a set of possible keys for use in personalization of an electronic component, especially a chip card so that protection against side channel attacks or crypto analysis is improved

Patent number:	FR2836312
Publication date:	2003-08-22
Inventor:	BRIER ERIC; CLAVIER CHRISTOPHE
Applicant:	GEMPLUS CARD INT (FR)
Classification:	
- international:	***H04L9/06;*** **H04L9/06**; (IPC1-7): H04L9/28; G06K19/07
- european:	H04L9/00; H04L9/06; H04L9/06C; H04L9/30
Application number:	FR20020001883 20020215
Priority number(s):	FR20020001883 20020215

Also published as:

WO03071733 (A1)
AU2003222888 (A

Abstract of **FR2836312**

Method for generation of secret secure keys for a cryptographic algorithm has the following steps: extraction of a set of possible keys; extraction of a sub-set of keys; and generation of secret keys from a sub-set of keys. The invention also relates to a corresponding device for personalization of an electronic component using a secret key chosen at random from a sub-set of possible keys using the inventive method.